UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,667	02/05/2004	Mukesh Kumar Singh	TI-35979	5588

23494 7590 09/20/2007

TEXAS INSTRUMENTS INCORPORATED
P O BOX 655474, M/S 3999
DALLAS, TX 75265

EXAMINER	
DEBNATH, SUMAN	
ART UNIT	**PAPER NUMBER**
2135	

NOTIFICATION DATE	DELIVERY MODE
09/20/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

uspto@ti.com
uspto@dlemail.itg.ti.com

mN

Office Action Summary	Application No.	Applicant(s)	
	10/772,667	SINGH, MUKESH KUMAR	
	Examiner	Art Unit	
	Suman Debnath	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/05/2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/02/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-14 are pending in this application.

Claim Objections

2. Claims 1 and 13 are objected to for lack of antecedent basis:

Claim 1 recites "the determinant" in line 3.

Claim 13 recites "the determinant" in line 2 and "the results" in line 4.

Appropriate correction and/or clarification is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 9-12 are rejected under 35 U.S.C. 102(e) as being anticipated by Chung (Pub. No.: US 2003/0016823 A1).

5. As to claim 9, Chung discloses a method of encryption, comprising: (a) preprocessing an input message wherein said preprocessing includes a permutation of the message (FIG. 2, [0011]); and (b) encrypting said preprocessed message with a

block-based encryption method which has blocks smaller than said message (FIG. 2, [0011]).

6. As to claim 10, Chung discloses wherein: (a) said permutation of step (a) of claim 9 is generated by a hash of said input message ([0036]).

7. As to claim 11, Chung discloses wherein: (a) said permutation of step (a) of claim 9 is generated by a random sequence ([0036]).

8. As to claim 12, Chung discloses wherein: (a) said encryption of step (b) of claim 9 is a public key encryption ([0036]).

9. Claims 13-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Bohannon et al. (Patent No.: US 6,901,145 B1) (hereinafter "Bohannon").

10. As to claim 13, Bohannon discloses a method of decrypting, comprising: (a) computing the determinant of a matrix-based encrypted message matrix (col. 10, lines 64-67 to col. 11, lines 1-61); (b) decrypting said determinant (col. 10, lines 64-67 to col. 11, lines 1-61); and (c) multiplying said matrix by the results of step (b) (col. 10, lines 64-67 to col. 11, lines 1-61).

11. As to claim 14, Bohannon discloses wherein: (a) when said matrix-based encrypted message of step (a) of claim 13 had preprocessing including a permutation, applying the inverse of said permutation to the results of step (c) of claim 13 (col. 11, lines 25-35).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bohannon and further in view of Slavin (Pub. No.: US 2004/0062390 A1).

14. As to claim 1, Bohannon discloses a method of encryption, comprising: (b) computing the determinant of said matrix (col. 10, lines 64-67 to col. 11, lines 1-61); (c) encrypting said determinant; and (d) multiplying said matrix by said encrypted determinant (col. 10, lines 64-67 to col. 11, lines 1-61).

Bohannon doesn't explicitly disclose (a) partitioning an input message into matrix elements. However, Slavin discloses (a) partitioning an input message into matrix elements ([0055], see also [0033], [0044]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Bohannon as taught by Slavin in order to "perform both encryption and decryption with relatively fewer calculations, which can result in a higher encryption/decryption throughput, and/or lower power consumption (Slavin, [0015])".

15. As to claim 2, Bohannon discloses further comprising: (a) prior to step (a) of claim 1, preprocessing said input message wherein said preprocessing includes a permutation of the message (col. 10, lines 64-67 to col. 11, lines 1-61).

16. As to claim 3, Bohannon discloses wherein: (a) said permutation of step (a) of claim 2 is generated by a hash of said input message (col. 10, lines 64-67 to col. 11, lines 1-61).

17. As to claim 4, Bohannon disclose wherein: (a) said permutation of step (a) of claim 2

is generated by a random sequence (col. 10, lines 64-67 to col. 11, lines 1-61).

18. As to claim 5, Bohannon discloses wherein: (a) said preprocessing of step (a) of claim 2 includes exclusive ORing said message after permutation with generators of said permutation (col. 10, lines 64-67 to col. 11, lines 1-61).

19. As to claim 6, Bohannon discloses wherein: (a) said encrypting of step (c) of claim 1 is public-key encryption (col. 10, lines 64-67 to col. 11, lines 1-61).

20. As to claim 7, Bohannon discloses wherein: (a) said public-key encryption is RSA (col. 10, lines 64-67 to col. 11, lines 1-61).

21. As to claim 8, Bohannon discloses wherein: (a) said partitioning of step (a) of claim 1 first fills the principal diagonal of said matrix (col. 10, lines 64-67 to col. 11, lines 1-61).

22. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Conclusion

23. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100